بسمه تعالی

سازمان بورس واوراق بهادار
SECURITIES & EXCHANGE ORGANIZATION

تاریخ:.....
شماره:.....

اطلاعیه

شماره اطلاعیه: ۱۲۰۳۰۰۷۵-۱۴۰۰/۰۳/۱۹

صادرکننده: مدیریت نظارت بر نهادهای مالی

موضوع: سند جامع الزامات امنیت اطلاعات بازار سرمایه

مخاطبین: کلیه نهادهای مالی

با سلام و احترام؛

به اطلاع می‌رساند، با توجه به افزایش تهدیدات سایبری بر روی زیرساخت‌ها و سامانه‌های بازار سرمایه با هدف اختلال در سرویس‌دهی به مشتریان، سرقت و افشای اطلاعات مشتریان و شرکت، اختلال در عملکرد معاملاتی شرکت، الزامات امنیت اطلاعات بازار سرمایه به شرح زیر جهت بهره‌برداری ابلاغ می‌شود. کلیه نهادهای مالی موظف‌اند، الزامات زیر را رعایت نمایند:

۱. پیاده‌سازی الزامات اطلاعات بازار سرمایه(نسخه ۴,۰)
۲. انجام تست نفوذ سامانه‌های بر بستر اینترنت، توسط شرکت‌های مورد تایید افتا
۳. به‌روزرسانی سیستم عامل‌ها، تجهیزات امنیت و شبکه و سیستم‌های کاربران
۴. بازنگری کلیه دسترسی‌های مدیریتی (پنل ادمین، SSH، RDP و از این قبیل) به سامانه‌ها، سرویس‌های زیرساختی، تجهیزات شبکه و امنیت و سیستم عامل‌ها به صورت مستقیم از شبکه اینترنت (استفاده از VPN با پروتکل‌های L2TP/SSTP)
۵. اطمینان از بسته بودن تمام پورت‌های غیر ضروری سرویس‌ها
۶. پایش مستمر ترافیک شبکه و لاگ‌های سرویس‌های حیاتی
۷. بازنگری امن‌سازی‌های انجام شده در سطح تجهیزات، سرویس‌ها، پایگاه داده‌ها و سیستم عامل‌ها
۸. اعمال افزونگی در کلیه لایه‌های زیر ساختی سرویس‌دهی به منظور جلوگیری از قطع شدن سرویس
۹. محافظت از سامانه‌های موجود در بستر اینترنت با استفاده از تجهیزات WAF/IPS اختصاصی
۱۰. تغییر کلیه کلمات عبور پیش‌فرض بر روی کلیه سیستم‌ها و سامانه‌ها

تهران – میدان ونک – خیابان ملاصدرا- شماره ۱۳
تلفن:۸۸۶۷۹۵۵۸
فاکس:
صندوق پستی: ۶۳۶۶-۱۹۳۹۵

13 Mollasadra Ave. Vanak Sq .Tehran.

۱۱ عدم استفاده از کاربران اشتراکی در سیستم‌ها، سرویس‌ها و سامانه‌ها

۱۲ تفکیک صحیح منطقی شبکه کاربران داخلی به VLAN ها و Zoneها و استفاده از فایروال در شبکه داخلی برای ایجاد دسترسی‌های لازم

۱۳ عدم وجود دسترسی Any از شبکه کلاینت‌ها به سمت اینترنت

۱۴ عدم اعتماد به شبکه‌های متصل بالادستی و همکار

۱۵ حذف دسترسی‌های موقتی اعطا شده در سرویس‌ها و شبکه

۱۶ نصب آنتی ویروس با لایسنس اصلی برای تمامی کامپیوترهای کاربران و سرورها

۱۷ پشتیبان‌گیری از داده‌ها و نگهداری حداقل یک نسخه پشتیبان در خارج از شبکه داخلی به صورت امن

۱۸ اطمینان از انتقال داده‌های محرمانه برروی بسترهای ارتباطی از جمله اینترنت با استفاده از پروتکل‌های امن و به صورت رمز شده(مانند SSL)

۱۹ عدم publish سامانه تستی و غیر عملیاتی بر روی اینترنت

۲۰ انجام اسکن آسیب‌پذیری شبکه و رفع موارد آسیب‌پذیر به صورت دوره‌ای

۲۱ حذف دسترسی به پنل‌های مدیریتی سامانه‌ها در بستر اینترنت

۲۲ اطلاع‌رسانی کلیه موارد مشکوک به مرکز نظارت بر امنیت اطلاعات بازار سرمایه

لازم به ذکر است، مرکز نظارت بر امنیت اطلاعات بازار سرمایه مسئول پاسخگویی در خصوص موارد فوق می‌باشد.

میثم فدائی واحد

مدیریت نظارت بر نهادهای مالی